8-16-1996

Meeting the Controls Challenges of New Information Technologies

Barbara J. Bashein
College of Business Administration, California State University San Marcos, bashein@csusm.edu

Jane B. Finley
Massey Graduate School of Business, Belmont University, finleyj@pcmail.belmont.edu

M. Lynne Markus
Programs inInformation Science, The Claremont Graduate School, markusm@cgs.edu

Meeting the Controls Challenges of New Information Technologies

Barbara J. Bashein
College of Business Administration, California State University San Marcos,
San Marcos, CA 92096-0001, 619-750-4232, bashein@csusm.edu
Jane B. Finley
Massey Graduate School of Business, Belmont University,
Nashville, TN 37212-3757, 615-385-6478, finleyj@pcmail.belmont.edu
M. Lynne Markus
Programs in Information Science, The Claremont Graduate School,
Claremont, CA 91711-6190, 909-607-3151, markusm@cgs.edu

Organizations frequently implement new information technologies to streamline operations and to improve control over cost and other important performance metrics. However, new information technologies can also pose significant control risks. Consider these examples.

Many larger organizations today are replacing their legacy mainframe systems with systems based on client/server architecture. Most observers agree that the security and backup features of the client/server systems are primitive compared to the sophistication possible with mature mainframe technology. Some organizations may be tempted to ignore controls due to the difficulty of implementing them in the new environment; other control risks may be introduced inadvertently.

Data warehouses are designed to facilitate data access and use. Yet by consolidating previously distributed data and by providing easy-to-use access tools, organizations may be opening themselves up to unauthorized access and misuse both by insiders and by outsiders.

New communications technologies, such as mobile computing, Lotus Notes, the Internet, and the World Wide Web, also present control risks. Many companies are starting to use the Internet (or Intranet) to distribute company-confidential information such as directories, organization charts, employee benefits information, and product manuals.

Evidence is accumulating that organizations need to be concerned simultaneously with both the security risks and the reliability issues associated with new technologies. On the security front, they need to be concerned both with accidental risk and with intentional threats. To deal effectively with technology-related risks, organizations need plans to prevent risks and plans to recover from accidents or attacks. Unfortunately, research shows that most organizations only develop control policies and procedures after there has been some sort of threat or event that greatly raises managers' consciousness of risk. Clearly, more research is needed both to raise awareness and to identify the approaches most likely to succeed in controlling the risks associated with the new information technologies.

Background and Research Questions

In the fields of accounting and financial management, *internal control* is understood as a process, effected by an entity's board of directors, managers, and other personnel, designed to provide reasonable assurances in three categories:

1. Effectiveness and efficiency of operations

2. Reliability of financial reporting

3. Compliance with applicable laws and regulations

As previously noted, information technology poses various threats or *risks* to an organization's internal control. A few such risks are well researched in the IS literature, although they are not generally conceptualized as risks to *organizational control*. These well researched risks include: the risk of software development failure and risks to security and privacy. By reviewing a large and diverse body of literature in the IS, accounting, organizational behavior, and general management fields, we developed a framework of the control risks posed by information technology and the categories of practices that might be effective in controlling them.

New information technologies pose a variety of risks to internal control, including:

1. *Competitive risk*-failure due to misperceptions of what is required to give competitive advantage or due to competitors responding more swiftly than expected

2. *Contingency risk*-accidents and natural disasters; e.g., floods, breaks in power lines

3. *Control system design risk*-errors inadvertently built into software or omitted error-checking features

4. *Development risk*-cost overruns, schedule delays

5. *External fraud, theft, or crime risk*-unknown outsiders perpetrating willful damage on or through technology; e.g., hackers who steal computer time, information, and funds

6. *Internal abuse risk*-trusted people (employees and business partners) intentionally using technology in ways contrary to the organization's interests

7. *Nonuse and unintentional misuse risk*-employees or business partners who are unable to or refuse to use the technology or use the technology incorrectly

8. *Reputation risk*-negative reactions by the public-at-large or key stakeholders to a company's information technology initiatives

9. *Technical risk*-computing hardware or software that does not work or vendors who fail to support the technology acceptably

Effective practices to manage the control risks of new information technologies fall into several overlapping categories:

1. *Awareness training*-face-to-face discussions and presentations about control risks

2. *Belief systems*-widely-held values and beliefs pertaining to the risk; e.g., "confidentiality of our customer information is sacred"

3. *Boundary systems*-strong statements of "what not to do" in the risk domain; e.g., "never give out passwords"

4. *Diagnostic controls*-performance measurement and monitoring related to the risk; e.g., periodic internal security reviews

5. *Operational controls*-formal processes and procedures not embedded in the technology; e.g., required authorizations of single-source vendors over a certain dollar limit

6. *Social controls*-peer pressure that employees exert when a coworker violates stated or unstated policies

7. *Technological and automated controls*-controls built into the information technologies; e.g., automated spending limits in purchasing support systems

The three major research questions addressed in this study are:

- What are the best practices for managing the internal control risks due to new information technologies?
- What external or internal factors strengthen or weaken the effectiveness of the best practices?
- What are the most successful strategies for implementing the best practices?

Methodology

This study lends itself to the case study research method. Our research design involves six in-depth case studies of companies reputed to be leaders in implementing and managing new information technologies. The particular technologies of interest include: data warehouses; enterprise client/server systems; the Internet, Intranet, and World Wide Web; and workflow systems.

Five of the six planned case study sites have already agreed to participate: American Standard Companies, BankAmerica Corporation, Microsoft Corporation, Norrell Corporation, and USAA. We have developed a detailed case study protocol, outlining the specific research questions to be answered and the sources of information for each. The sections of the protocol are:

1. *Case study background*-basic information about the industry, the case study company, the relevant strategic challenges, the particular new information technology in this case site, and the reasons for implementing it

2. *Control risks posed the new information technology*-the specific class(es) of risk posed by the new technology for the case site

3. Effective control practices-the practices used by the case site and the effectiveness of these practices; additional practices that might prove effective will also be identified

4. *Implementation strategies*-the history and process of change in the case site's control practices; additional change management activities that might prove effective will also be identified

5. *Best control practices*-for each case site, the best practices will be synthesized, and the effectiveness of the practice attributed to the content of the control practices, the process of control implementation, or both

Potential data sources for answering the research questions include: internal company documents, public information (e.g., news accounts), and interviews with CIOs, CFOs, technology project managers, security officers, auditors, and vendors, and other organizational informants.

After the individual case studies are complete, we will conduct a thorough cross-case analysis. This analysis will address similarities and differences in control risks and control practices and will determine the factors most likely to explain the similarities and differences. If this step is omitted or poorly performed, case studies, no matter how detailed, often yield limited value. A systematic cross-case analysis provides greater confidence in the recommendations by showing how general they are and by showing the particular conditions under which the recommendations can be expected to apply.

Expected Contributions

The research summarized here is expected to contribute practical guidelines about an issue of great importance to virtually all organizations that use information technology today. In particular, we aim to shed light on the following questions:

- How can organizations maximize the benefits of new information technologies without increasing the control risks to unacceptable levels?
- What control risks do organizations perceive to be associated with the new information technologies, and how are organizations addressing these risks?
- What implementation strategies are most effective in introducing and enforcing controls of technology-related risks?